Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **Bc. Hajšo Patrik** **Oponent:** **Ing. Adam Němec**

Studijní program: **Informační technologie**
Studijní obor/Specializace: **Kybernetická bezpečnost**
Akademický rok: **2023/2024**

Téma diplomové práce: **Nastroj pro identifikaci kryptografických a kódovacích algoritmů**

Hodnocení práce:
Diplomová práce studenta Patrika Hajša na téma identifikace kryptografických a kódovacích algoritmů, má velmi dobře zpracovanou dokumentaci. Vyskytuje se zde pár stylistických chyb, které ale nijak nesnižují její kvalitu.
Praktická část práce bohužel vykazuje několik nedostatků, ke kterým mám výhrady. Jako první bych vytkl celkovou náročnost samotné práce. Například hashovací funkce diplomant analyzuje pouze pomocí základních regulárních výrazů, proto aplikace velmi často vrátí i 7 možných hashovacích algoritmů na jeden hash. Kromě toho bych diplomantovi vytkl i samotný zdrojový kód aplikace. Soubor CodeWindow.py obsahuje značné množství duplicitního kódu, který by mohl být optimalizován s využitím funkcí. V kódu se také nacházejí zakomentované části, které by měly být v případě nepoužívání smazány. Seznamy regulárních výrazů v souboru HashWindow.py by mohly být pro snazší správu umístěny v externím souboru, například v JSON formátu. Celkově aplikace bohužel nefunguje zcela spolehlivě. Analýza kódování Base58 v některých případech selhávala a vracela hlášku "neplatný výsledek". V jiných případech aplikace nedokázala správně identifikovat hash SHA256.
Celkově je práce Patrika Hajša velmi zajímavá a poměrně funkční. Jen by bylo vhodné ji dostatečně otestovat, lépe zpracovat zdrojový kód aplikace a trochu více se věnovat samotné problematice identifikaci kryptografických algoritmů.

Otázky k obhajobě:
1. Proč je v práci zakomentovaný regulární výraz pro hash CRC-32?
2. Jakým způsobem probíhalo testování aplikace?

Celkové hodnocení práce:
Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně, F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou diplomovou práci doporučuji k obhajobě a navrhuji hodnocení

C - dobře.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Datum Podpis oponenta diplomové práce